(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295341 A
(43)申请公布日 2017.01.04

(21)申请号 201610655252.7

(22)申请日 2016.08.11

(71)申请人 浪潮电子信息产业股份有限公司
地址 250101 山东省济南市高新区浪潮路1036号

(72)发明人 李超

(74)专利代理机构 济南信达专利事务所有限公司 37100
代理人 姜明

(51)Int.Cl.
G06F 21/56(2013.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

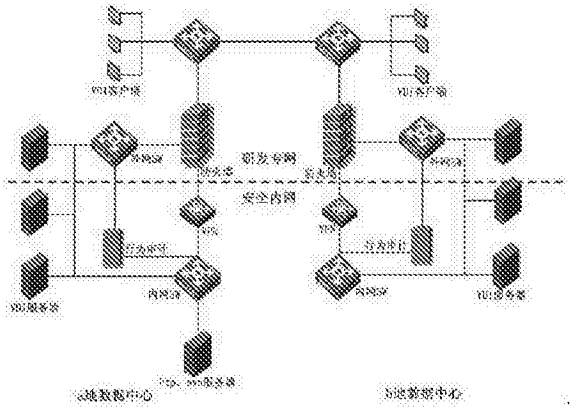
权利要求书1页 说明书2页 附图2页

(54)发明名称

基于虚拟化的企业数据中心安全解决方法

(57)摘要

本发明提供一种基于虚拟化的企业数据中心安全解决方法，涉及虚拟化和企业数据中心网络领域；由防火墙隔离终端与VDI Server之间的数据传输只允许VDI协议报文通过，研发专网到安全内网之间仅允许VPN通道数据可通过，VDI Server需要同时连接研发专网和安全内网，并且VDI Server与研发专网之间只通过VDI内部协议进行信息传输；整个数据中心中只有VDI Server同时接入到研发专网和安全内网中，研发专网用户访问数据需使用VDI远程虚拟桌面进行。本发明可保护企业重要数据不被泄露和丢失，节能减排，降低企业成本。



CN 106295341 A

1.基于虚拟化的企业数据中心安全解决方法,其特征在于,

整个数据中心的内部数据交互在安全环境内网进行,安全环境内网中的服务器以及各种应用服务器都通过内部交换机连接;由防火墙隔离终端与VDI Server之间的数据传输只允许VDI 协议报文通过,而研发专网到安全内网之间仅允许VPN通道数据可通过,禁用研发专网对安全内网的直接访问;同时, VDI Server需要同时连接研发专网和安全内网,并且VDI Server与研发专网之间只通过VDI内部协议进行信息传输;整个数据中心中只有VDI Server同时接入到研发专网和安全内网中,研发专网用户访问数据需使用VDI远程虚拟桌面进行。

2.根据权利要求1所述的方法,其特征在于,

VDI 客户端即研发专网通过Security Service即转网段连接到Connect通过认证后登陆到虚拟机,Security Service同时提供PCoIP连接服务,虚拟机中不留任何访问外网的接口,虚拟机中不留任何访问外网的接口,两地的虚拟机只能通过安全内网网段访问ftp、svn。

3.根据权利要求2所述的方法,其特征在于,

VDI客户端与VDI服务器之间传输的数据是图像和指令码,防火墙隔离,允许VDI客户端只访问VDI Server;

通过行为审计和防火墙网络数据的采集、分析、识别,实时动态监测通信内容、网络行为,发现和捕获各种敏感信息、违规行为,全面记录网络系统中的各种会话和事件。

基于虚拟化的企业数据中心安全解决方法

技术领域

[0001] 本发明涉及虚拟化和企业数据中心网络领域，尤其涉及一种基于虚拟化的企业数据中心安全解决方法。

背景技术

[0002] 目前，随着企业对信息化建设的越来越重视，企业的运维成本也随着传统PC的不断增多而增加，传统PC也暴露出了各种问题和弊端。

[0003] 数据安全性问题：传统PC缺乏保护措施，极易造成公司关键信息的外泄，从而给公司带来重大的损失；另外，当出现故障或断电情况容易导致传统PC的系统损坏、数据丢失等致命问题。

[0004] 移动办公问题：对于经常出差的人员，时常需要把数据从办公台式机拷贝到移动设备上，无法做到在任何时间、任何地点使用同一办公桌面。

[0005] 设备更新问题：传统PC更新速度较快，一般使用年限在3~5年。设备更新不仅带来大量的电子垃圾，而且需要投入大量购置费用和维护费用。

[0006] 维护量大问题：传统PC经过一段时间的使用后，硬件故障和软件故障逐渐增多，系统维护工作量大且缺乏统一集中的管理，计算机维护人员需要花费大量时间进行此项工作。

发明内容

[0007] 本发明提出了一种基于虚拟化的企业数据中心安全解决方法，针对企业中传统PC存在的问题，保护企业重要数据不被泄露和丢失，以及桌面的集中管理、统一配置和维护，节能减排，降低企业成本。

[0008] 本发明提出的是一种基于虚拟化的企业数据中心安全解决方法。此解决方案的思路是基于VMware 虚拟化技术，利用防火墙、VPN、行为审计等设备建立安全的数据中心及两地数据中心之间的通信，保护企业重要数据的安全。

[0009] 整个数据中心的内部数据交互在安全环境内网进行，安全环境内网中的服务器以及各种应用服务器，如SVN和FTP都通过内部交换机连接，可以保证内部通信的需要。由防火墙隔离终端与VDI Server之间的数据传输(只允许VDI 协议报文通过)，而研发专网到安全内网之间仅允许VPN通道数据可通过，禁用研发专网对安全内网的直接访问。同时，为实现研发专网到安全内网的受限访问，VDI Server需要同时连接研发专网和安全内网，并且VDI Server与研发专网之间只通过VDI内部协议进行信息传输。整个数据中心中只有VDI Server同时接入到研发专网和安全内网中，研发专网用户访问数据需使用VDI远程虚拟桌面进行。

[0010] VDI 客户端即研发专网通过Security Service即转网段连接到Connect通过认证后登陆到虚拟机，Security Service同时提供PCoIP连接服务，虚拟机中不留任何访问外网的接口，虚拟机中不留任何访问外网的接口，两地的虚拟机只能通过安全内网网段访问

ftp、svn。

针对传统PC暴露出的各种问题，提出基于虚拟化的企业数据中心安全解决方法，该方法具有以下优点：

1、VDI客户端与VDI服务器之间传输的数据是图像和指令码，不传输实质数据，避免被侦听。防火墙隔离，允许VDI客户端只访问VDI Server，避免对其它信息系统形成安全威胁。

[0011] 2、通过VDI Server设置安全策略，使U盘数据单向可读，保证资料不被拷贝；设置单向粘帖，避免数据从VDI客户端漏。禁止终端PC与虚拟桌面的文件共享，禁止打印。

[0012] 3、虚拟机模板化，只安装与工作生产相关的程序，可简化维护、提升安全。

[0013] 4、通过行为审计和防火墙网络数据的采集、分析、识别，实时动态监测通信内容、网络行为，发现和捕获各种敏感信息、违规行为，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全事件的准确全程跟踪定位。

附图说明

[0014] 图1是数据中心网络topo图；

图2是 VMware View架构图。

具体实施方式

[0015] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明做进一步地详细描述：

如图1所示，企业a、b两地的数据中心网络topo图，该网络topo主要包含防火墙、行为审计、VDI服务器、VPN等；其中VDI服务器包括：View Composer、View Manager、vCenter、AD等组件。VDI服务器有2个网卡， 其中一个位于研发专网，另一个在安全内网，AD域管理，vCenter，Composer，Connect等都要位于内网，只有security service使用研发专网，数据不可以从安全内网导出。a、b两地通过VPN建立IP-SEC 隧道形成虚拟局域网，两地网络通讯加密，防止网络侦听、假冒。通过防火墙安全策略限制越权访问：防火墙安全策略采用进入、输出物理口限定，允许当地VDIClient访问当地VDI Server，允许a、b两地VDI Server访问svn，vpn与防火墙相结合，保障只有VDI服务器可以访问到SVN。行为审计设备通过旁路监听的方式接入网络，在不影响网络正常使用的情况，既可以监听VDI Server与安全专网的通信，又可以同时监听研发专网与VDI Server之间的访问。

[0016] 简单流程介绍：VDI 客户端(研发专网)通过Security Service(转网段)连接到Connect通过认证后登陆到虚拟机，Security Service同时提供PCoIP连接服务，虚拟机中不留任何访问外网的接口，虚拟机中不留任何访问外网的接口，a、b两地的虚拟机只能通过安全内网网段访问ftp、svn等。

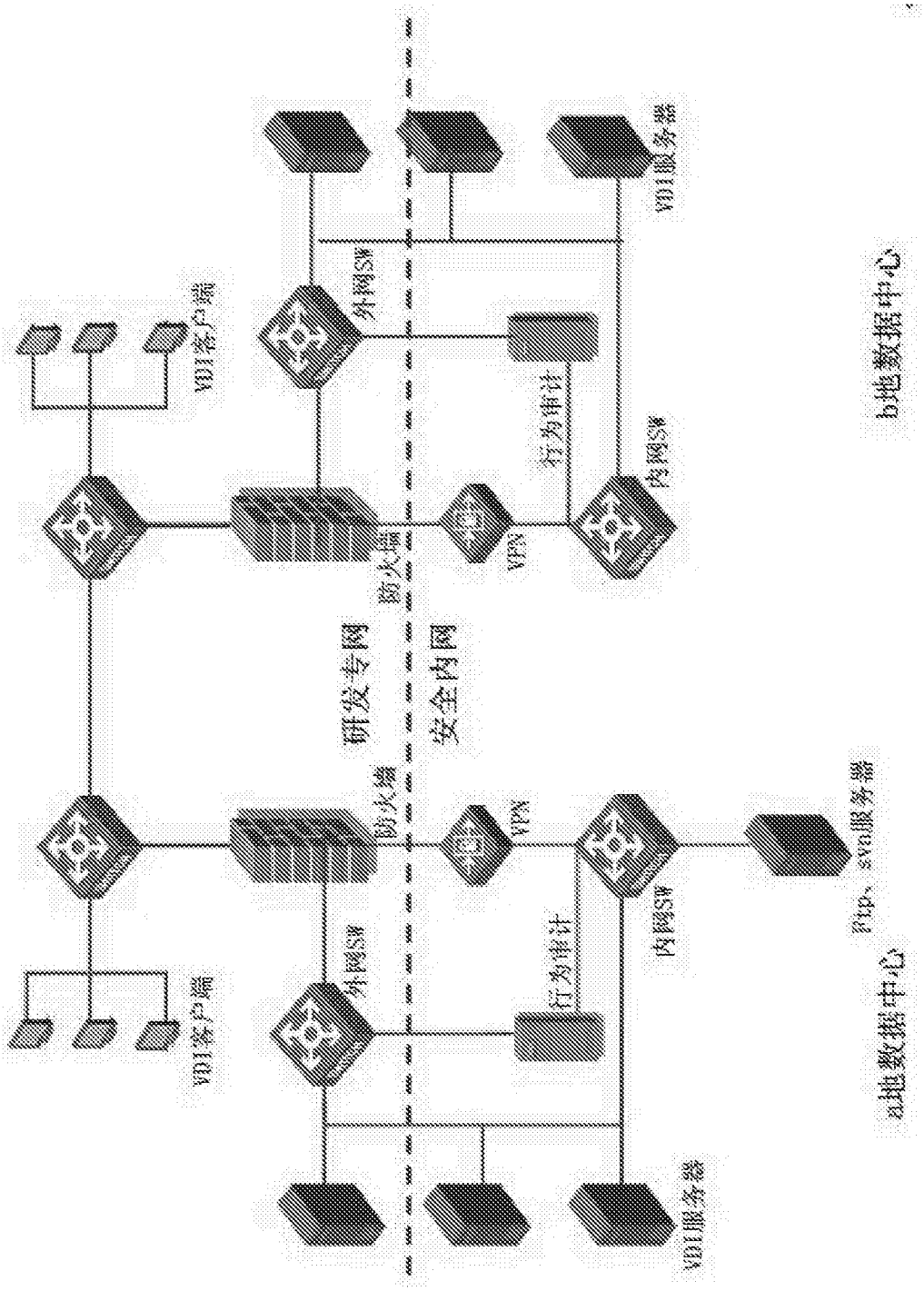

VDI客户端
外网SW
VDI服务器
行为审计
内网SW
b地数据中心
防火墙
VPN
研发专网
安全内网
防火墙
VPN
内网SW
ftp、svn服务器
外网SW
行为审计
VDI客户端
a地数据中心
VDI服务器

图1

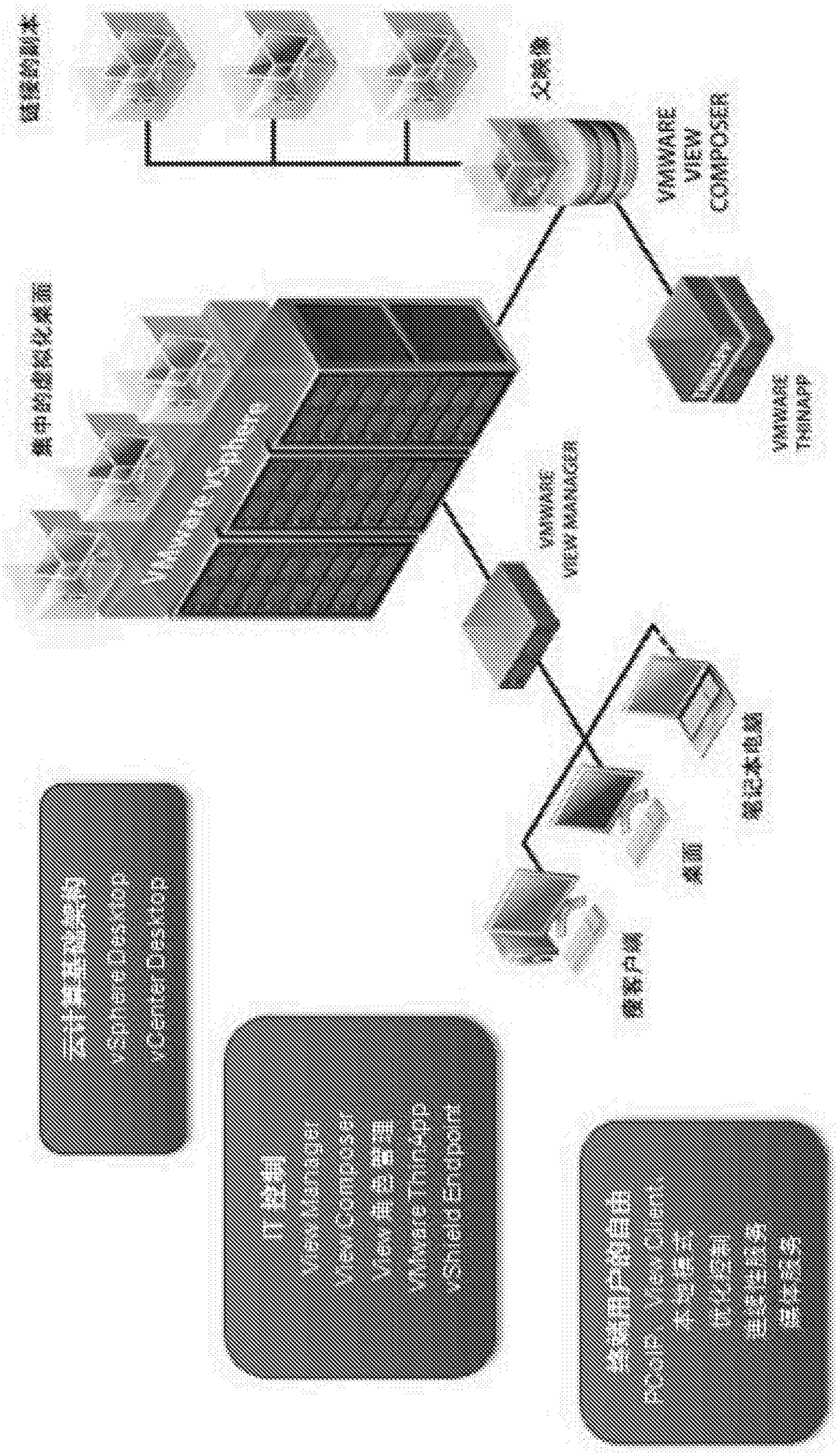

VMWARE VIEW COMPOSER
VMWARE VIEW MANAGER
VMWARE THINAPP
VMware vSphere
vSphere Desktop
vCenter Desktop
IT 控制
View Manager
View Composer
vShield Endpoint

图2